anand guru

SOC EXPERTS

Interview Questions on
Analysis & Incident Response

Anand Guru

Security+ | CySA | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

How do you handle a malware alert?

Malware Alert

Gather Information

- Hostname
- User
- File Name
- File Path
- Malware Name
- Malware Category
- File Hash
- AV Action

AV Action

Deleted

1. Identify the Source of the malware
   - Check for emails received by the user 2-4 hours before the malware detection
   - Check for all the website the user has visited in last 1 hour
   - Check the possibility of malware detection on USB (by Drive letter in file path)
2. Research on the malware (to see if it is targeted)
3. Check if the file hash appears else where in the network

- Email – Take permission and delete all the email from the sender/subject line or mails having the attachment
- Web – Block the URL on Proxy and IP address on the firewall
- USB – Educate the user about the malware, issue warning

Not Deleted/Not Quarantined

1. Raise and incident to manually remove the malware
2. Continue Analysis and keep adding notes to the incident
3. Check if AV has up-to-date signatures
4. Check for any file modification, registry modifications, user account creations, privilege escalation and audit logs of the affected host

Manually remove the malware and rescan the host

How do you remove a malware manually?

Step 1: Download Process Explorer and enable VirusTotal integration

Step 2: Run Process Explorer and look for the malicious process

Step 3: Identify the path of the process

We cannot delete the file from the path as it is currently running. If we try killing the process it comes up again immediately.

Step 4: Boot the machine in safe mode

In safe mode only minimum required windows process will run, there by preventing the malware from running.

Step 5: Delete the malicious file from the identified path

Step 6: Boot in standard mode and run a full scan

Should the machine be removed from the network?

Depends on the host in question, if it is a critical server and there are no redundant servers, we cannot isolate it from the network

How do you work on a Phishing Alert?

Phishing Mail Reported

Open the Mail in .MSG format

1. Is the mail from public domain (like gmail, yahoo etc.)?
2. Is the domain name misspelled (like amazone.com)?
3. Is the email poorly written (grammar mistakes, incorrect use of words etc.)? Attackers do this to bypass standard filtering.
4. Does the email create a sense of urgency?
5. Right click on link and 'Copy link Address' and paste the URL on a notepad.
6. Copy the Internet Header
7. Copy the email to a sandbox and download attachments

1. Submit the URL to www.urlvoid.com and check the reputation.
2. Check the domain in WHOIS lookup to identify the IP address of the domain. Check the reputation of the IP at www.ipvoid.com
3. Paste the Internet Header to www.mxtoolbox.com (Analyze Headers)
   - Check for DMARC compliance
   - Check for SPF Alignment and Authentication
   - Check the DKIM Alignment and Authentication
4. Check the Return-Path
5. Check the reputation of IP address and domain names that appear in the header information

- Block the domain at the Email Gateway
- Block associated IPs at Firewall
- If there are other copies of email in other users mailbox, take permission to delete them
- Educate the user of the techniques used in the phishing email

How do you investigate a Brute-force Attack?

Brute-force Alert
Gather Information
Valid User?
Has Higher Privileges
Source IP(s)
Destination IP(s)
User Name(s)
Logon Type
Login Failure Reason
1. Check if the Source IP is Local or Remote?
2. What is the destination IP?
3. How any source IP s are involved?
4. What is the frequency of the attempts?
5. Failure Reason (User Account disabled OR password incorrect or Account Locked etc.)
• Temporarily disable the user account
• Ask user to change the password
• If external IP is involved, block it on Firewall

How do you analyze a DOS attack?

DOS Alert
Gather Information
1. Source IP (s)
2. Targeted IP
Affected Services is Critical or Public Facing?
1. Access the service as a user to see if it is still up and running
2. Run 'netstat –an' to check if there are several WAIT connections
3. Run continuous pings to see if there are any packet drops
4. Check the bandwidth consumption on network monitoring tools (PRTG, Nagios)
5. If the intensity is too high open the Bridge call
• Open a bridge call with the network team, ISP, application team, SOC lead/manager and Server team
• Temporarily add more servers to load balance
• Reduce the connection-wait-time
• Limit the No. of connection from an IP address
• Block the top 5 or 10 IPs that are aggressively involved in the attack
• Prepare to bring up the DR servers

anand guru

How to work on a Ransomware alert?

Ransomware Alert

Logic of the correlation rule will be based on some IOC of a Ransomware, so it is important to verify if the IOCs are reliable

Gather Information

1. Source IP (s)
2. IOCs (URL or Hash or IP address

1. Verify the credibility of the IOC. Use IBM Xforce or www.URLVoid.com to check the reputation and confidence level.
2. Gather information like IP address, track the host name (by DHCP logs).
3. Call the user and inform about the situation
4. Take remote and ensure the AV is running and has latest signatures.
5. Also, look for any indication of a ransomware attack (file extension, inaccessible files etc.)
6. If the alert is genuine, ask the user to disconnect from the network open a ticket and assign it to endpoint security team
7. Continue analysis to understand the source of the malware.
8. Look for any other infected machine with the help of IOC or source of malware.

- Identify the type of ransomware and the stage of encryption.
- If it is in the early stage of encryption, try to identify the process and kill it.
- DO NOT reboot the machine as it might render the machine useless
- If file are already encrypted try to look for decryption keys from reliable source (AV vendors)
- If it is a user machine, format it.
- If it is a server, format it and restore form the backup

anand guru

Explain the analysis for a SQL Injection Attack

SQL Injection Attack Alert

Usually IPS and WAF can report SQL Injection attempts

Gather Information

1. Source IP (s)
2. Log Source (IPS/WAF)
3. Severity

1. Check the reputation of the IP address
2. Check if this IP address was involved in any recon activity on our servers
3. Look for suspicious events on the database (like configuration changes, strange queries, DROP statements etc.)
4. Check to see if there is any anomaly in SELECT statements.

- Raise a ticket to block the IP on the firewall.
- Raise a ticket to expedite the Patching process on the target server.

anand guru

Walk through the steps you follow to analyze 'Communication to Bad Reputation IP' alert.

Possible Botnet Activity Alert

Gather Information

1. Source IP
2. Destination IP
3. Destination Port
4. Log Source
5. Device (Firewall/IPS/Proxy) Action

1. Check the reputation of the public IP. Check its history and what kind of malicious activity (scanning, C&C, spam etc.) it is involved in.
2. Check the destination port. If it is other than 80 and 443 and is allowed by Firewall → Raise a ticket and assign it to firewall team to block the traffic.
3. Check if the source host has latest AV signatures.
4. Identify the process involved in generating the traffic on the machine (use the tool TCPLogView)
5. Check if the IP address is associated with any domain name or malware distribution (www.virustotal.com or www.threatcrowd.org)
6. Get the associated file hashes and check if they ever appeared in your network.
7. Take the associated URL/Domain name and see if they were visited by any users.

- If the traffic is allowed, block the IP at Firewall level
- If it is done by a malware (botnet) remove it manually and run a full scan on the machine.
- Ensure all the configurations on the affected system are intact
- Ensure the associated URLs are blocked
- Feed the associated file hashes to SIEM to detect and other attacks

anand guru

‘IPS alert on a Vulnerable Host’ rule is triggered, how do you analyze it?

IPS alert on a Vulnerable Host Alert

Gather Information

1. Source IP
2. Destination IP
3. Destination Port
4. IPS Alert Name/Severity

1. Check the reputation of the source IP.
2. Check the IPS Alert and understand what it means and the severity of the alert.
3. See if there is an associated vulnerability (exploit signature of IPS) to the alert.
4. Research on the vulnerability using the CVE number. Look for affected OS, application and their versions.
5. Check if the target server is using the vulnerable version.

- Raise a ticket to block the IP on the firewall.
- Raise a ticket to expedite the Patching process on the target server.

Steps you take to analyze 'Unknown Process Detected' alert.

Unknown Process Detected Alert

Gather Information

1. Source IP
2. Host
3. Process Name
4. Process Hash
5. Process path

1. Verify if it is a known malicious process by submitting the Hash to www.virustotal.com
2. If it is not a malicious process check with the user if he has installed any new software/application and ask for business justification
3. If the user is not aware of the running process, the new process has be analyzed (malware analysis) to check if it is malicious

- Raise a ticket to block the IP on the firewall.
- Raise a ticket to expedite the Patching process on the target server.

anand guru

Full course on Udemy

IT & Software › Network & Security › Cyber Security

SOC Analyst (Cybersecurity) Interview Questions and Answers

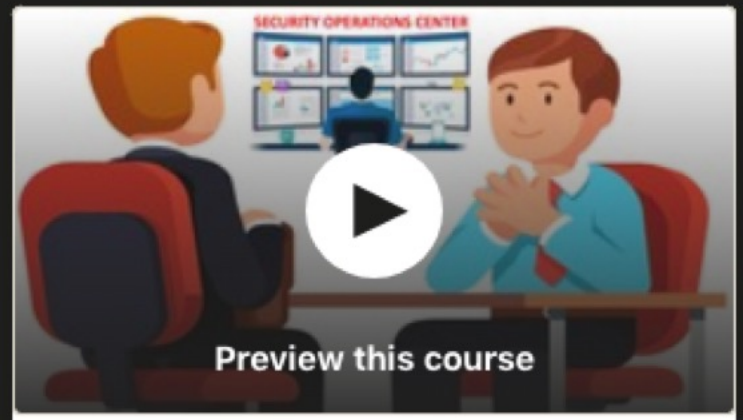
Clear your next SOC interview with ease with these 300+ interview question asked during most SOC Analyst Interview

Bestseller 4.6 ★★★★½ (106 ratings) 2,248 students

Created by Anand Guru

Last updated 5/2020 English English

Wishlist Share Gift this course



₹455 ~~₹1,280~~ 64% off

5 hours left at this price!

Add to cart

Buy now

30-Day Money-Back Guarantee

What you'll learn

- ✓ Security Analyst/SOC Analyst interview questions and how to answer them
- ✓ Tricky questions and how to answer them
- ✓ Scenario based questions
- ✓ SOC Analyst Training
- ✓ Wide range of topics covered in a SOC Interview
- ✓ How to answer experience related questions
- ✓ Ready-to-use sample CVs for SOC Analyst role

This course includes:

- 2.5 hours on-demand video
- 2 articles
- 8 downloadable resources
- Full lifetime access
- Access on mobile and TV
- Certificate of completion